

TOP SECRET//COMINT//NOFORN NATIONAL SECURITY AGENCY CENTRAL SECURITY SERVICE

FORT GEORGE G. MEADE, MARYLAND 20755-6000

23 February 2009

MEMORANDUM FOR THE CHAIRMAN, INTELLIGENCE OVERSIGHT BOARD

THRU: Assistant to the Secretary of Defense (Intelligence Oversight)

SUBJECT: (U//FOUO) Report to the Intelligence Oversight Board on NSA Activities - INFORMATION MEMORANDUM

(U//FOUC) Except as previously reported to you or the President, or otherwise stated in the enclosure, we have no reason to believe that any intelligence activities of the National Security Agency during the quarter ending 31 December 2008 were unlawful or contrary to Executive Order or Presidential Directive and thus should have been reported pursuant to Section 1.7.(d) of Executive Order 12333.

(U//FOUO) The Inspector General and the General Counsel continue to exercise oversight of Agency activities by inspections, surveys, training, review of directives and guidelines, and advice and counsel. These activities and other data requested by the Board or members of the staff of the Assistant to the Secretary of Defense (Intelligence Oversight) are described in the enclosure.

GEORGE ELLARD

Inspector General

VITO T. POTENZA General Counsel

(U//FOUO) I concur in the report of the Inspector General and the General Counsel and hereby make it our combined report.

KEITH B. ALEXANDER Lieutenant General, U. S. Army Director, NSA/Chief, CSS

Encl:

Quarterly Report

This document may be declassified and marked "UNCLASSIFIED//For Official Use Only" upon removal of enclosure(s)

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20320108

TOP SECRET//COMINT//NOFORN

1. (U//FOUO) Intelligence, counterintelligence, and intelligence-related activities that violate law, regulation, or policy substantiated during the quarter, as well as actions taken as a result of the violations.

(C) mitoling of local trials	ence Activitie) Intellige	(U)
------------------------------	----------------	-------------	-----

	(TS//SI// REL TO USA, FVEY	Unintentional collection	against United States	
	persons. This quarter, there	<u> </u>	•	
	analysts inadvertently targeted			
	while pursuing foreign intellige	nce tasking. All intercepts and	d reports have been deleted or	
b) (1)	destroyed as required by United	States SIGINT Directive (US	SID) SP0018.	
b)(3)-P.I	L. 86-36		(b) (1) (b) (3)-P.L. 86-36	
	(U) Unauthorized Targeting		(b) (3) -18 USC 798	
			(b) $(3) -50$ USC 3024(i)
//-	(TS//SI//NF) An NSA analyst v	<u> </u>	e number for collection on	
		the selector was foreign		
/	foreign intelligence target. This			
	The selector w		the analyst was paired with a from this violation (b) (1)	
	senior analyst for additional train	ining. No collection resulted i	rom this violation (b) (3)-P.L. 86	-36
	(TS//SI//REL TO USA, FVEY)		SA analyst improperly searched	
	for information on NSA a			
	appraisals. The violation was for		who provided	
	additional training to the analys		results, which were purged from	
	the NSA database		Jassans, water were purges now.	
(b) (1)				
(b) (3) -P.	(T\$/\si/NF)	an NSA		
1		ded the e-mail address of	in a query list of targeted	
//		his mistake the same day, and	the query was terminated with no	
//	results		(b)(3)-P.L. 86-36 (b)(3)-50 USC 3024(i)
//	/TC//CI//DEL TO LICA EVEV	On tors a serious sellenting		Τ,
//	were in the United States. In th		occurred while valid foreign targets	
	were in the Offited States. In th		selectors were not removed	
//			on was purged from NSA	
\	databases. The second instance		Selectors were deactivated	
,		•	but collection	
	occurred before		intercepts were purged from an	
	NSA database as they were iden		// No	
	reporting resulted from either v	iolation.	(b) (1)	
	and a various train		(b)(3)-P.L. 86-	.36
,	(TS//SI//NF)	NSA analysts learned of a	bollection	
and the same of th	violation. Analysts believe that	And the second s	records occurred	
(1) (1)		(b) (1)		
(b) (1) (b) (3) -	P.L. 86-36	(b) (3) -P.L. 86-36		
	50 USC 3024(i)	(b) (3)-18 USC 798 (b) (3)-50 USC 3024(i)	Derived From: NSA/CSSM 1-52	
		(, (,	Dated: 20070108	
			Declassify On: 39480914	

Unfortunately, all related collection was purged from NSA databases in 2004.
The details of the violation are still being researched. The NSA/CSS Office of the Inspector
General (OIG) will track this action and report the results. (b) (1) (b) (3)-P.L. 86-36
(TS//SI//REL) On an NSA analyst learned that foreign targets were
targeted e-mail selectors were detasked,
and collection was purged from an
NSA database. When confirming the detasking the analyst found that the
selectors had not been removed from The cause of the
problem was software-related. The selectors were removed
No collection resulted because had not been conducted from
(b) (1)
(U) Database Queries (b) (3)-P.L. 86-36 (b) (3)-P.L. 86-36 (b) (3)-50 USC 3024(i)
(S//SI//REL_TO USA, FVEY) On occasions, NSA analysts constructed poor database queries.
In of the occasions, collection resulted from the overly broad or incomplete queries. All
resulting collection was deleted. The remaining incidents did not result in collection. No
reports were issued.
reports were insuca.
(TS//SI//REL TO USA, FVEY) Additionally, on occasions, NSA analysts failed to verify that
targets were located outside the United States before conducting database queries. In of the
instances, the oversights resulted in collection.
All queries were terminated and when collection occurred, the data was deleted.
No reporting occurred. (b) (1) (b) (3) -P.L. 86-36
/b) /3\\\ 19 HGC 700
(U) Detasking Delays (b) (3) -50 USC 3024(i)
(TS//SI//NF) A valid foreign target traveled to the United States and
before the target's selector was detasked. A detasking request was submitted
on the
United States. The detasking did not occur until after the target returned
overseas. This violation was caused by an inefficient process for detasking. To lessen the
risk of future violations of this type, analysts are now required to
Collection associated with this violation was purged from NSA
databases
(b) (1) (b) (3) -P 1 86-36

	(U) Destruction Delays
	(S//SI//REL TO USA, FVEY) Human error caused a delay in deleting an NSA database. an NSA analyst submitted a purge request with the intent of deleting collection from He mistakenly believed that the request would effect purging for was deleted from the when the mistake was found.
	(S//SI//REL_TO USA, FVEY) Unintentional dissemination of U.S. identities. There wereinstances in which SIGINT analysts disseminated communications to, from, or about U.S. persons while pursuing foreign intelligence tasking this quarter. All data have been deleted or destroyed as required by USSID SP0018. Inof theinstances, SIGINT products were cancelled because they contained the identities of U.S. persons, organizations, or entities. The reports were either not reissued or were reissued with proper minimization. (b) (3)-P.L. 86-36 (b) (3)-18 USC 798
-	(S//SI//NF) an NSA analyst included information from SIGINT about a
	NSA although, within NSA, the is not part of the
	SIGINT production chain. Additionally, the same unminimized and unevaluated traffic was forwarded to assigned to NSA. The (b)(3)-P.L. 86-36 was not authorized to receive unminimized and unevaluated SIGINT. In both
(b) (1) (b) (3) -P.L.	instances, the disseminated data was destroyed.
-	e-mailed a briefing that included identities of a U.S. and U.S. and U.S. to the
	when the analyst recognized the mistake, she directed destruction of the brief by the as she applied for an identity release The had no record of the e-mailed briefing to destroy.
	(S//SI//RELTO_USA, FVEY) the name of a U.S. person was included
	in e-mail tips to elements inside and outside the SIGINT Production Chain. The violation was recognized the same day. The e-mails were recalled and a destruction notification was forwarded to all addressees.
-	(TS//SI//REL-TO USA, FVEY) an NSA analyst included U.S.
	The NSA analyst forwarded
	the analyst noticed that he had not minimized the U.S. identifiers. He directed and confirmed the destruction of the charts by
	(b)(1) (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36 (b)(3)-18 USC 798 (b)(3)-50 USC 3024(i)
	(L) (3) -30 OGC 3024(I)

(U) The Foreign Intelligence Surveillance Act (FISA)	(b)(1)
(U) Business Records Order	(b)(3)-P.L. 86-36 (b)(3)-50 USC 3024(i)
(TS//SI//REL TO USA, FVEY) On 28 October 2008, an NSA a FISA (BRFISA) data for telephone selectors without author because the analyst used an old version of the navigation software. The analyst updated the navigation soft other analysts were reminded to update their software. No data were issued. (TS//SI//REL TO USA, FVEY) On 31 October 2008, passed a mistyped phone number to an NSA analyst.	are, tware on 9 December 2008, and a was retained, and no reports
resulted in the targeting of an number in Busines. 3 November 2008 until 5 January 2009. All related call chaining	s Records FISA data from
(TS//SI//NF) On 15 December 2008, an NSA analyst improperl U.S. telephone number. Although the number was associated v been approved for call chaining in the BRFISA data. The analymust be sought for BRFISA call chaining. No data w issued.	y accessed BRFISA data for a with a foreign target, it had not
(U// FOUO) Although the following violation occurred during t reporting timeframe, the incident is significant enough to warra	
Court (FISC) that NSA had been using an "alert list" to BRFISA metadata against phone numbers associated witargets that NSA had tasked for SIGINT collection. Alt reported to the Court that the alert list consisted of number determined that a reasonable articulable suspicion (RAS) were related to a terrorist organization associated with the vast majority of selectors on the subjected to a RAS determination. The circumstances is are still under research. The NSA/CSS OIG will track to results.	compare incoming ith counterterrorism hough the Agency had bers for which NSA had bers for which NSA had been sisted that the numbers (b) (1) (b) (3)-P.L. 86-36 (b) (3)-50 USC 3024(1) currounding this incident
(U) Pen/Trap Order	
(U) Nothing to report.	
(U) The Protect America Act (PAA)	
(U) Nothing to report.	

	(U) The FISA Amendments Act	
	(S//SI//NF) A target selector was not detasked during a target's	isit
	to the United States. an NSA analyst requested detasking of	
	target's e-mail selector on The selector was removed	
	but the analyst detasking process	1
	Resulting collection was purged from the NSA databases. No reporting occurred)(1) b)(3)-P I 96-36
	Resulting Collection was purged from the NSA databases. No reporting occurred.	o) (3)-50 USC 3024(i)
	(TS//SI//REL TO USA, FVEY) During a tasking record review NS	SA
		s due
	diligence found that the analyst mistakenly selected FISA Amendments Act (FAA)	
	Certification instead of the FAA Certification. No colle occurred between when the selectors were tasked and	when
	the selector was detasked, and no reports were issued.	(b) (1)
		(b)(3)-P.L. 86-36
•	(TS//SI//REL TO USA, FVEY) A target with U.S. and citizenship was incorrectly	1
	under the FAA Certification in violate	1
	FAA section 702. A U.S. person may not be tasked pursuant to section 702 of the Act. NSA analyst did not notice the target's dual citizenship when the e-mail selector was tas	
	Resulting collection was purged from NSA databases	KCU.
		ftware
	processing error prevented the deletion of the data	(b)(1) (b)(3)-P.L. 86-36
	(TS//SI//NF) an FAA-authori zed target was active on an e-mail ad	dress
	Collection was purged from NSA databa	t t
	but a software processing error prevented the deletion of the d	
	The problem was isolated and the data was purged To ensure no other purging requests were affected.	
	system administrators re-processed all purging requests dating back to	
	(TS//SI//NF) an FAA-tasked e-mail account selector associated v	
	the United States. The selector was not detas	a de la companya de
/	until because of a database software problem, which was corrected of the target selector to be detasked was in the	on (b)(3)-P.L. 86-36 elated
/	collection was purged from NSA databases No repo	
/	occurred. (b) (1)	
/		.L. 86-36
/	(TS//SI//REL TO USA, FVEY) NSA analysts learned that a target	selector
/	was not an NSA analyst requested detasking of the target's e-mail select	or on
	L H	
/	The analyst submitted the detasking request, but	failed to
	notify the detasking office and the need to bypass the standard	
	detasking process. Resulting collection was purged from the NSA databases on No reporting occurred.	」 /
	(b) (1) (b) (3) -PL. 86-36	
(b)(1) (b)(3)-P.L.		
(b) (3) -18 U (b) (3) -50 U	SC 798	$\sqrt{}$
(5) (5) -50 0	5	(b)(1) (b)(3)-P.L. 86-36
		(b)(3)-50 USC 3024(i)

	MINIT//NIOEODNI

(b)	(1)		
(b)	(3)-P.L.	86-36	
(h)	(3) -50 HS	20 3024/11	

(TS//SI//NF) an NSA analyst learned that an e-mail selector tasked for collection under the FAA Certificate did not meet the FAA tasking standards.	
The selector was detasked As a result of this incident, the tasking	
process has been changed to reduce the risk of future mistakes. Applicable selectors are now	
No collection or reporting occurred.	
(S//SI//NF) On an NSA analyst detasked a telephone selector of a target	
active in the United States, but failed to The process failure was corrected on when the oversight	
was identified. Collection was purged from NSA databases on	٦
was identified. Conceitor was purged from NSA databases on	_
(TS//SI//REL TO USA, FVEY) Human error resulted in collection of a target's communication	2
while he was in the United States from	,
White he was in the cinted states from	\neg
The second error occurred when a	/
analyst	1
noted the target as outside the United States	1
All related collection was purged from NSA databases	
(b)(3)-P.	L. 86-36
) USC 3024(i
(TS//SI//NF)	Ц
(TS//SI//REL TO USA, FVEY) Human error caused a day detasking delay, which resulte	-d
in collection while the target selector was active in the United States. The request to terminate	
the FAA-authorized collection was submitted on but the selector was not	
detasked until The analyst left on and did not return until	
at which time the selector was detasked, and the resulting collection was purged from a NSA	
database onNo reporting occurred on the unauthorized collection.	
(b) (1) (b) (3) -P.L. 86-36 (b) (3) -P.L. (b) (b) (3) -P.L. (b) (b) (3) -P.L. (b) (b) (3) -P.L.	
(b) (3)-18 t	
(b) (3) $-P.L.$ 86-36 (b) (3) -50 t	JSC 3024(i)
(U) Unintentional Dissemination	
an NGA States a mailed FIGA callested	
(S//SI//RELTO USA, FVEY) an NSA analyst e-mailed FISA-collected	
data to who was not authorized to receive the FISA data. U.S. person information	11
was not included in the e-mail. The analyst, who misunderstood information sharing policy, confirmed the destruction of the data by the	
commined the destruction of the data by the	

	TOP SECRET//COMINT//NOFORN	(b)(1) (b)(3)-P.L. 86-36 (b)(3)-50 USC 302
terminated	error resulted in the targeting of e-mail sele Although the selectors were removed from NSA analysts did not annotate th Consequently, the selectors was destroyed, and	at the selectors were ectors remained active
terminated	Although the selectors were removed from NSA analysts did not annotate the Consequently, the selectors was destroyed, and	at the selectors were ectors remained active
(U) Computer Netwo	ork Exploitation	(b) (3) -P.L. 86-36 (b) (3) -18 USC 798 (b) (3) -50 USC 3024(
-(TS//SI//REL TO US	SA, FVEY)	(5) (3),-30 050 3024(
(TS//SI//NF)		
(TS//SI//REL TO US targeted e-mail addr States,	, ,	yst learned that a the target was in the United
<u> </u>		// -

-TOP SECRET//COMINT//NOFORN-

(b)(1) (b)(3)-P.L. 86-36 (b)(3)-50 USC 3024(i)

(U)	Intelligence-related	Activities
-----	----------------------	------------

(TS//SI//NF) NSA/CSS analysts found that e-mail selectors this quarter. No collection occurred.		
NSA/CSS analysts found that e-mail selectors this quarter. No collection occurred. (C//REL TO USA, FVEY) Although not violations of E.O. 12333 and related directives, NSA/CSS reports instances in which database access was not terminated when access was no longer required. Once identified, accesses were revoked. In another instance, a work study employee was issued a database account in error. Accounts are only to be granted to analysts on a need-to-know basis, which was not the case with the high school work study employee. The student had not received training, and it was not activated before the account was terminated. The Branch Chief who authorized the account was counseled on the importance of understanding work roles before submitting individuals for database accounts. (b)(1) (b)(3)-P.L. (b)		
NSA/CSS analysts found that e-mail selectors this quarter. No collection occurred. (C//REL TO USA, FVEY) Although not violations of E.O. 12333 and related directives, NSA/CSS reports instances in which database access was not terminated when access was no longer required. Once identified, accesses were revoked. In another instance, a work study employee was issued a database account in error. Accounts are only to be granted to analysts on a need-to-know basis, which was not the case with the high school work study employee. The student had not received training, and it was not activated before the account was terminated. The Branch Chief who authorized the account was counseled on the importance of understanding work roles before submitting individuals for database accounts. (b)(1) (b)(3)-P.L. (b)		
NSA/CSS analysts found that e-mail selectors this quarter. No collection occurred. (C//REL TO USA, FVEY) Although not violations of E.O. 12333 and related directives, NSA/CSS reports instances in which database access was not terminated when access was no longer required. Once identified, accesses were revoked. In another instance, a work study employee was issued a database account in error. Accounts are only to be granted to analysts on a need-to-know basis, which was not the case with the high school work study employee. The student had not received training, and it was not activated before the account was terminated. The Branch Chief who authorized the account was counseled on the importance of understanding work roles before submitting individuals for database accounts. (b)(1) (b)(3)-P.L. (b)		
NSA/CSS analysts found that e-mail selectors this quarter. No collection occurred. (C//REL TO USA, FVEY) Although not violations of E.O. 12333 and related directives, NSA/CSS reports instances in which database access was not terminated when access was no longer required. Once identified, accesses were revoked. In another instance, a work study employee was issued a database account in error. Accounts are only to be granted to analysts on a need-to-know basis, which was not the case with the high school work study employee. The student had not received training, and it was not activated before the account was terminated. The Branch Chief who authorized the account was counseled on the importance of understanding work roles before submitting individuals for database accounts. (b)(1) (b)(3)-P.L. (b)	When collection occurred, it was purged from NS	SA databases. (b) (3) -50 U
NSA/CSS analysts found that e-mail selectors This quarter. No collection occurred.		
this quarter. No collection occurred. (C//REL TO USA, FVEY) Although not violations of E.O. 12333 and related directives, (b) (3) = P NSA/CSS reports instances in which database access was not terminated when access was no longer required. Once identified, accesses were revoked. In another instance, a work study employee was issued a database account in error. Accounts are only to be granted to analysts on a need-to-know basis, which was not the case with the high school work study employee. The student had not received training, and it was not activated before the account was terminated. The Branch Chief who authorized the account was counseled on the importance of understanding work roles before submitting individuals for database accounts. (E) (1) (b) (3) = P. L. (b)	(TS//SI//NF)	
this quarter. No collection occurred. (C//REL TO USA, FVEY) Although not violations of E.O. 12333 and related directives, (b) (3) = P NSA/CSS reports instances in which database access was not terminated when access was no longer required. Once identified, accesses were revoked. In another instance, a work study employee was issued a database account in error. Accounts are only to be granted to analysts on a need-to-know basis, which was not the case with the high school work study employee. The student had not received training, and it was not activated before the account was terminated. The Branch Chief who authorized the account was counseled on the importance of understanding work roles before submitting individuals for database accounts. (E) (1) (b) (3) = P. L. (b)	NCA/CCC analysts found that \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	
(C//REL TO USA, FVEY) Although not violations of E.O. 12333 and related directives, (b) (3) -P NSA/CSS reports instances in which database access was not terminated when access was no longer required. Once identified, accesses were revoked. In another instance, a work study employee was issued a database account in error. Accounts are only to be granted to analysts on a need-to-know basis, which was not the case with the high school work study employee. The student had not received training, and it was not activated before the account was terminated. The Branch Chief who authorized the account was counseled on the importance of understanding work roles before submitting individuals for database accounts. (TS//SI//REL TO USA, FVEY) was inappropriately forwarded to was inappropriately forwarded to the non-SIGINT analysts. The recipients destroyed the data (b) (1) (3) -P. L. 86-36 (TS//SI//REL TO USA, FVEY) analyst wrongfully shared his NSA Network (NSANet) account password with another SIGINT analyst assigned to The analyst was relieved of his duties and transferred to the could share his NSANet for training purposes. The analyst was relieved of his duties and transferred to the county of the data did not contain U.S. person information. An analyst at Fort Gordon recognized the mistake. The e-mail was recalled, and destruction of the data was confirmed by telephone. The OIC completed refresher training on SIGINT dissemination.	NSA/CSS alialysts found thate-mail selectors	
NSA/CSS reports instances in which database access was not terminated when access was no longer required. Once identified, accesses were revoked. In another instance, a work study employee was issued a database account in error. Accounts are only to be granted to analysts on a need-to-know basis, which was not the case with the high school work study employee. The student had not received training, and it was not activated before the account was terminated. The Branch Chief who authorized the account was counseled on the importance of understanding work roles before submitting individuals for database accounts. (ED) (1) (ED) (3) - P. L. (ED) ((b) (1)
no longer required. Once identified, accesses were revoked. In another instance, a work study employee was issued a database account in error. Accounts are only to be granted to analysts on a need-to-know basis, which was not the case with the high school work study employee. The student had not received training, and it was not activated before the account was terminated. The Branch Chief who authorized the account was counseled on the importance of understanding work roles before submitting individuals for database accounts. (Eb) (3) -P. L. (Eb) (3)		
study employee was issued a database account in error. Accounts are only to be granted to analysts on a need-to-know basis, which was not the case with the high school work study employee. The student had not received training, and it was not activated before the account was terminated. The Branch Chief who authorized the account was counseled on the importance of understanding work roles before submitting individuals for database accounts. (b) (1) (b) (3)-P.L. (b) (3		
analysts on a need-to-know basis, which was not the case with the high school work study employee. The student had not received training, and it was not activated before the account was terminated. The Branch Chief who authorized the account was counseled on the importance of understanding work roles before submitting individuals for database accounts. (b) (1) (b) (3)-P.L. (c) (b) (3)-P.L. (c) (b) (3)-P.L. (c) (c) (d) (d) (d) (d) (d) (d) (d) (d) (d) (d		
employee. The student had not received training, and it was not activated before the account was terminated. The Branch Chief who authorized the account was counseled on the importance of understanding work roles before submitting individuals for database accounts. (b) (3)-P.L. (c) (3)-P.L		
terminated. The Branch Chief who authorized the account was counseled on the importance of understanding work roles before submitting individuals for database accounts. (b) (1) (b) (3) -P.L. (b) (3	•	· ·
understanding work roles before submitting individuals for database accounts. (b)(3)-P.L. (b)(3)-P.L. (b)(3)-P.L. (b)(3)-P.L. (b)(3)-P.L. (b)(3)-P.L. (b)(3)-P.L. (c)(3)-P.L. (c)(3)-P.L. (d)(3)-P.L. (d)(3)-P.L. (e)(3)-P.L. (e)(4)-P.L.		
was inappropriately forwarded to analysts failed to follow NSA policy and guidance for dissemination of SIGINT technical information and sent the data to the non-SIGINT analysts. The recipients destroyed the data (E)(1) (E)(3)-P.L. 86-36 (TS//SI//REL TO USA, FVEY) analyst wrongfully shared his NSA Network (NSANet) account password with another SIGINT analyst assigned to The analyst mistakenly believed he could share his NSANet for training purposes. The analyst was relieved of his duties and transferred to the (TS//SI//REL TO USA, FVEY) the Officer-in-Charge (OIC) of a forwarded unminimized and unevaluated SIGINT to all-source analysts outside the SIGINT production chain. The data did not contain U.S. person information. An analyst at Fort Gordon recognized the mistake. The e-mail was recalled, and destruction of the data was confirmed by telephone. The OIC completed refresher training on SIGINT dissemination. (TS//SI//REL TO USA, FVEY)		riduals for detabase accounts
was inappropriately forwarded to analysts failed to follow NSA policy and guidance for dissemination of SIGINT technical information and sent the data to the non-SIGINT analysts. The recipients destroyed the data (b) (1) (b) (3)-P.L. 86-36 (TS//SI//REL TO USA, FVEY) analyst wrongfully shared his NSA Network (NSANet) account password with another SIGINT analyst assigned to The analyst mistakenly believed he could share his NSANet for training purposes. The analyst was relieved of his duties and transferred to the (TS//SI//REL TO USA, FVEY) (TS//SI//REL TO USA, FVEY) the Officer-in-Charge (OIC) of a forwarded unminimized and unevaluated SIGINT to all-source analysts outside the SIGINT production chain. The data did not contain U.S. person information. An analyst at Fort Gordon recognized the mistake. The e-mail was recalled, and destruction of the data was confirmed by telephone. The OIC completed refresher training on SIGINT dissemination.	understanding work foles before submitting marv	, (D) (J) [: II.
was inappropriately forwarded to analysts failed to follow NSA policy and guidance for dissemination of SIGINT technical information and sent the data to the non-SIGINT analysts. The recipients destroyed the data (b) (1) (b) (3) -P.L. 86-36 (TS//SI//REL TO USA, FVEY) analyst wrongfully shared his NSA Network (NSANet) account password with another SIGINT analyst assigned to The analyst mistakenly believed he could share his NSANet for training purposes. The analyst was relieved of his duties and transferred to the (TS//SI//REL TO USA, FVEY) the Officer-in-Charge (OIC) of a forwarded unminimized and unevaluated SIGINT to all-source analysts outside the SIGINT production chain. The data did not contain U.S. person information. An analyst at Fort Gordon recognized the mistake. The e-mail was recalled, and destruction of the data was confirmed by telephone. The OIC completed refresher training on SIGINT dissemination.	(TS//SI//REL-TO-USA, FVEY)	
analysts failed to follow NSA policy and guidance for dissemination of SIGINT technical information and sent the data to the non-SIGINT analysts. The recipients destroyed the data (TS//SI//REL TO USA, FVEY) analyst wrongfully shared his NSA Network (NSANet) account password with another SIGINT analyst assigned to The analyst mistakenly believed he could share his NSANet for training purposes. The analyst was relieved of his duties and transferred to the (TS//SI//REL TO USA, FVEY) the Officer-in-Charge (OIC) of a forwarded unminimized and unevaluated SIGINT to all-source analysts outside the SIGINT production chain. The data did not contain U.S. person information. An analyst at Fort Gordon recognized the mistake. The e-mail was recalled, and destruction of the data was confirmed by telephone. The OIC completed refresher training on SIGINT dissemination.		NSA
(TS//SI//REL_TO USA, FVEY) analyst wrongfully shared his NSA Network (NSANet) account password with another SIGINT analyst assigned to		nd guidance for dissemination of SIGINT
(TS//SI//REL TO USA, FVEY) analyst wrongfully shared his NSA Network (NSANet) account password with another SIGINT analyst assigned to The analyst mistakenly believed he could share his NSANet for training purposes. The analyst was relieved of his duties and transferred to the the Officer-in-Charge (OIC) of a forwarded unminimized and unevaluated SIGINT to all-source analysts outside the SIGINT production chain. The data did not contain U.S. person information. An analyst at Fort Gordon recognized the mistake. The e-mail was recalled, and destruction of the data was confirmed by telephone. The OIC completed refresher training on SIGINT dissemination.	technical information and sent the data to the non	-SIGINT analysts. The recipients destroyed the
analyst wrongfully shared his NSA Network (NSANet) account password with another SIGINT analyst assigned to	data (b) (1)	T 0.0
analyst wrongfully shared his NSA Network (NSANet) account password with another SIGINT analyst assigned to The analyst mistakenly believed he could share his NSANet for training purposes. The analyst was relieved of his duties and transferred to the the Officer-in-Charge (OIC) of a forwarded unminimized and unevaluated SIGINT to all-source analysts outside the SIGINT production chain. The data did not contain U.S. person information. An analyst at Fort Gordon recognized the mistake. The e-mail was recalled, and destruction of the data was confirmed by telephone. The OIC completed refresher training on SIGINT dissemination.		D. 00-30
analyst assigned to The analyst mistakenly believed he could share his NSANet for training purposes. The analyst was relieved of his duties and transferred to the the Officer-in-Charge (OIC) of a forwarded unminimized and unevaluated SIGINT to all-source analysts outside the SIGINT production chain. The data did not contain U.S. person information. An analyst at Fort Gordon recognized the mistake. The e-mail was recalled, and destruction of the data was confirmed by telephone. The OIC completed refresher training on SIGINT dissemination.		CANI-A
share his NSANet for training purposes. The analyst was relieved of his duties and transferred to the (TS//SI//REL_TO USA, FVEY) the Officer-in-Charge (OIC) of a forwarded unminimized and unevaluated SIGINT to all-source analysts outside the SIGINT production chain. The data did not contain U.S. person information. An analyst at Fort Gordon recognized the mistake. The e-mail was recalled, and destruction of the data was confirmed by telephone. The OIC completed refresher training on SIGINT dissemination. (TS//SI//REL_TO USA, FVEY)		
the Officer-in-Charge (OIC) of a forwarded unminimized and unevaluated SIGINT to all-source analysts outside the SIGINT production chain. The data did not contain U.S. person information. An analyst at Fort Gordon recognized the mistake. The e-mail was recalled, and destruction of the data was confirmed by telephone. The OIC completed refresher training on SIGINT dissemination. (TS//SI//REL_TO USA, FVEY)		
(TS//SI//REL_TO USA, FVEY) the Officer-in-Charge (OIC) of a forwarded unminimized and unevaluated SIGINT to all-source analysts outside the SIGINT production chain. The data did not contain U.S. person information. An analyst at Fort Gordon recognized the mistake. The e-mail was recalled, and destruction of the data was confirmed by telephone. The OIC completed refresher training on SIGINT dissemination.		myst was reneved of his duties and transferred to
forwarded unminimized and unevaluated SIGINT to all-source analysts outside the SIGINT production chain. The data did not contain U.S. person information. An analyst at Fort Gordon recognized the mistake. The e-mail was recalled, and destruction of the data was confirmed by telephone. The OIC completed refresher training on SIGINT dissemination. (TS//SI//REL_TO USA, FVEY)		\
forwarded unminimized and unevaluated SIGINT to all-source analysts outside the SIGINT production chain. The data did not contain U.S. person information. An analyst at Fort Gordon recognized the mistake. The e-mail was recalled, and destruction of the data was confirmed by telephone. The OIC completed refresher training on SIGINT dissemination. (TS//SI//REL_TO USA, FVEY)	(TS//SI//REL_TO USA: FVEY)	the Officer-in-Charge (OIC) of a
production chain. The data did not contain U.S. person information. An analyst at Fort Gordon recognized the mistake. The e-mail was recalled, and destruction of the data was confirmed by telephone. The OIC completed refresher training on SIGINT dissemination. (TS//SI//REL_TO USA, FVEY)	()	
recognized the mistake. The e-mail was recalled, and destruction of the data was confirmed by telephone. The OIC completed refresher training on SIGINT dissemination. (TS//SI//REL_TO USA, FVEY)		• · · · · · · · · · · · · · · · · · · ·
telephone. The OIC completed refresher training on SIGINT dissemination. (TS//SI//REL_TO USA, FVEY)		
(TS//SI//REL_TO USA, FVEY)		·
· · · · · · · · · · · · · · · · · · ·	· / · <u> </u>	
learned that a analyst sought and	(TS//SI//REL TO USA, FVEY)	
y and the second		

(b)(3)-P.L. 86-36
received NSAdatabase access through his former NSA/CSS
organization. The had determined that database access was not needed in the analyst's
job. After three unsuccessful attempts to gain database access through the normal request
process, the analyst contacted his former duty station and was sponsored for access on
database access was terminated Additionally, from
found (b)(1) (b)(3)-P.L. 86-36
analyst and analysts sponsored for
database access by an organization not authorized to sponsor access within the
area of operational responsibility. Database access for the analysts was
terminated pending proper sponsorship.
/TC//CL//DEL_TO LICA -EVEVY Lost quester NCA reported de problem with the
(TS//SI//REL TO USA; FVEY) Last quarter NSA reported a problem with the
malfunctioned, and the
causing the retention of U.S. person information.
odification was added to extend
The NSA Office of General Counsel has provided retention guidance to the affected (b)(1)
organizations. (b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
2. (U// FOUO) NSA/CSS OIG Intelligence Oversight Inspections, Investigations,
and Special Studies.
(U// FOUO) During this quarter, the OIG reviewed various intelligence activities of the NSA/CSS to determine whether they had been conducted in accordance with applicable statutes, Executive Orders, Attorney General procedures, and Department of Defense and internal directives. With few exceptions, the problems uncovered were routine and showed that operating elements understand the restrictions on NSA/CSS activities.
(U// FOUO) (b)(3)-P.L. 86-36
(U// FOUO) A joint inspection found that the would benefit from documented and
communicated processes. The focus of thentelligence oversight program has been E.O. 12333 training, but not local incident handling procedures. Intelligence oversight training
for newcomers is at an 86 percent compliance rate, and 99 percent for annual E.O. 12333
refresher training. Although collectors, analysts, and supervisors are aware of the restrictions on
the collection, analysis, and dissemination of U.S. person information, local incident reporting
standards, and internal controls to track newcomer training and the use of sensitive NSA
databases are needed. The OIG will track corrective action through completion.
(U// FOUO) NSA Office of
(U// FOUO) An inspection found that the intelligence oversight within NSA's Office of is appropriately managed and compliant with standing regulations.

(U// FOUO) Alleged Unauthorized Disclosure of Classified Information and Misuse of the United States SIGINT Service (USSS).
(S//SI//REL TO USA, FVEY) The NSA/CSS OIG reported alleged unauthorized disclosure of classified information and misuse of the USSS last quarter. a Navy Cryptologist met with an uncleared Navy Family Readiness social worker and disclosed that he had targeted his ex-wife and other family members through his job. An OIG inquiry found no evidence to support the sailor's claim.
(U) Congressional, IOB, and DNI Notifications.
(U) Nothing to report.
3. (U) Substantive Changes to the NSA/CSS Intelligence Oversight Program.
(U) Nothing to report.
4. (U) Changes to NSA/CSS published directives or policies concerning intelligence, counterintelligence, or intelligence-related activities and the reason for the changes.
(U) Nothing to report.
5. (U) Procedures governing the activities of Department of Defense (DoD) intelligence components that affect U.S. persons (DoD Directive 5240.1-R, Procedure 15) Inquiries or Matters Related to Intelligence Oversight Programs.
(U) Nothing to report.